510, 606

/510606

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
23 octobre 2003 (23.10.2003)

PCT

(10) Numéro de publication internationale
WO 03/088612 A2

(51) Classification internationale des brevets[7] : H04L 29/06

(21) Numéro de la demande internationale :
PCT/FR03/01169

(22) Date de dépôt international : 11 avril 2003 (11.04.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
02/04840 12 avril 2002 (12.04.2002) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **THOMSON LICENSING S.A.** [FR/FR]; 46, quai Alphonse Le Gallo, F-92100 Boulogne Billancourt (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **ANDREAUX, Jean-Pierre** [FR/FR]; 20, rue de Lorgeril, F-35000 Rennes (FR). **DIEHL, Eric** [FR/FR]; La Buzardière, F-35340 Liffré (FR). **DURAND, Alain** [FR/FR]; 79, rue de Dinan, F-35000 Rennes (FR).

(74) Mandataire : **BERTHIER, Karine**; Thomson, 46, quai Alphonse Le Gallo, F-92648 Boulogne Cedex (FR).

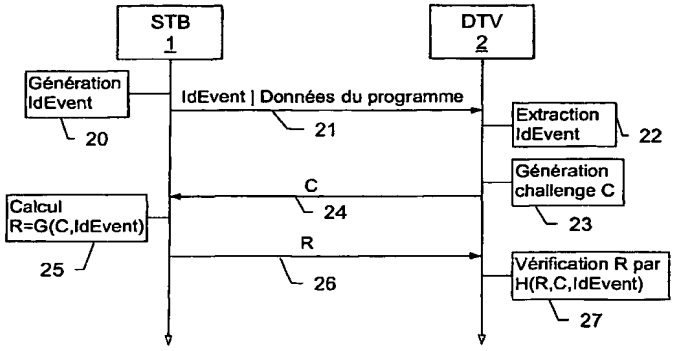
(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK,

[Suite sur la page suivante]

(54) Title: METHOD FOR THE ANONYMOUS AUTHENTICATION OF A DATA TRANSMITTER

(54) Titre : PROCEDE D'AUTHENTIFICATION ANONYME D'UN EMETTEUR DE DONNEES



20...GENERATION IDEVENT
25...CALCULATION R=G(C,id EVENT)
21...id EVENT PROGRAM DATA
22...EXTRACTION IDEVENT
23...GENERATION CHALLENGE C
27...CHECK R BY H(R,C,id EVENT)

(57) Abstract: The invention relates to a method whereby it can be checked whether data received by a receiver (2) has been sent by a transmitter (1, 3) authorised by a trusted third party, the transmitter and the receiver being connected to a digital network. An identifier (IdEvent) is associated with the data sent by the transmitter and, on receipt of the data by the receiver (2), the receiver generates a random number (C) and diffuses the same on the network. The transmitter that receives said random number calculates a response (R) by applying a first function (G) to the random number (C) and to the identifier (IdEvent), and sends said response (R) to the receiver which verifies the response received by applying a second function (H) to the response received, the random number (C) and the identifier (IdEvent). The first function (G) is delivered first to the transmitter by the trusted third party, and the second function (H) is a function for checking the result of the first function which is delivered first to the receiver by the trusted third party.

[Suite sur la page suivante]

WO 03/088612 A2